



# **COMPLYING WITH THE SOUTH CAROLINA INSURANCE DATA SECURITY ACT**

*A presentation by the South Carolina Department of Insurance | September 10, 2018*  
*South Carolina Bar Conference Center*



# Presentation Overview

**Greetings and Welcome**

**Overview of the Law**

**Regulatory, Legal and Compliance  
Issues**

**Reporting Requirements**  
*(Cybersecurity event notifications, Annual  
Reports, Certifications of Compliance to the  
SCDOI)*

**Frequently Asked Questions**

**Closing Remarks**



# **SOUTH CAROLINA INSURANCE DATA SECURITY ACT**

- **The National Association of Insurance Commissioners adopted the Insurance Data Security Model Law to establish standards for:**
  - **Data security;**
  - **Investigation; and**
  - **Notification of cyber security events.**
- **It is codified at Title 38, Chapter 99 of the South Carolina insurance laws with staggering effective dates.**
- **South Carolina was the first state to adopt the model. We anticipate that other states will enact the model in the near future.**



# Implementation of the South Carolina Insurance Data Security Act (SCIDSA)

- The South Carolina Insurance Data Security Act is based upon the NAIC Model (#686).
- The information security principles in the NAIC model and SCIDSA are similar to the information security principles in the Gramm-Leach-Bliley Act. They permit a licensee to pursue data security measures that are *appropriate for the size and complexity of licensee's business*.
- The SCDOI will not tell you what information security processes or procedures are appropriate for your business.
  - Your company's risk assessment should drive those decisions.
  - My Department has, and will continue to provide guidance in the form of interpretive bulletins, FAQs, presentations like this one and webinars.



# General Implementation Guidance

➤ **The following statutory requirements drive the Act's implementation:**

**Risk Assessment**

**Implementation of an Information Security Program**

**Development of Information Security Policies designed to protect the licensee's information systems and nonpublic information**

**Cybersecurity event Investigations and Notifications**

➤ **The Department has created a cybersecurity webpage, [www.doi.sc.gov/cyber](http://www.doi.sc.gov/cyber) where you will be able to find answers to questions about how the law will be implemented.**



# **Scrivener's Error**

- **The SCDOI will pursue correction of a scrivener's error in Section 38-99-70. This correction is consistent with the purpose and intent of the Act and does not alter its substance.**
- **States are trying to enact legislation that is substantially similar to the NAIC model to address concerns about a consistent regulatory approach. Therefore, no other changes are contemplated.**



# Future Implementation Guidance

Bulletin Number	Topic	Issue Date
2018-02	Overview of the South Carolina Insurance Data Security Act	June 14, 2018
2018-09	Notification Requirements Under the South Carolina Insurance Data Security Act	September 5, 2018
2018-TBD	Exemption Requirements under the South Carolina Insurance Data Security Act	TBD
2018-TBD	Guidance for Third Party Service Provider Programs	TBD





# **OVERVIEW OF THE LAW**

**Summary of Significant Components of the law**



# DISCLAIMER

- ❖ The information in this presentation was compiled from informational sources believed to be reliable and is intended for informational and for educational purposes only. This presentation contains general guidelines and information.
- ❖ When developing programs or policies, please review your company's information technology, data, risk assessment as well as other resources and consult with counsel of your choice for legal advice as to the appropriate compliance steps for your company.
- ❖ This presentation cannot be assumed to contain every acceptable information security compliance procedure for every South Carolina licensee. Nothing in this presentation should be interpreted as legal advice.
- ❖ **Attendees should know that this session is being video-recorded and will be published on the Department's website.**



## **SECTION 1 | PURPOSE**

- **The purpose and intent of the law is to establish standards for data security and standards for the investigation and notification to the director of a cybersecurity event applicable to licensees of the South Carolina Department of Insurance.**
- **This act does not create or imply a private cause of action for a violation *nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this act.***



# **APPLICATION OF THE LAW**

## **South Carolina Licensees**

**Any individual or nongovernmental entity *licensed, authorized to operate or registered or required to be licensed authorized or registered* under the state insurance laws.**

**Note: Licensees must require third party service providers performing services for a licensee comply with the provisions of the law.**

### **Examples include:**

- Domestic Insurers**
- Health maintenance organizations**
- Professional and surety bondsmen & runners**
- TPAs**
- Producers, Brokers, Adjusters, Managing General Agencies**



# KEY DEFINITION | ***Licensee*** | § 38-99-10

**A licensee is...**

***a person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State but does not include a purchasing group or a risk retention group chartered and licensed in a state other than this State or a licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction.***



# **KEY DEFINITION | Nonpublic Information | § 38-99-10(11)**

**Business related information of a licensee...**

- ...the tampering with which, or unauthorized disclosure, access, or use of which, would cause a material adverse impact to the business, operations, or security of the licensee;

**any information concerning a consumer which because of name, number, personal mark, or other identifier can be used to identify such consumer, in combination with any one or more of the following data elements:**

- (i) social security number;
- (ii) driver's license number or non-driver identification card number;
- (iii) account number, credit or debit card number;
- (iv) security code, access code, or password that would permit access to a consumer's financial account; or
- (v) biometric records;

**Any information from a health care provider except age or gender of consumer relating to:**

- the past, present or future physical, mental or behavioral health or condition of a consumer or a member of the consumer's family;
  - the provision of health care to a consumer; or
  - payment for the provision of health care to a consumer.



# KEY DEFINITIONS | **Cybersecurity Event** | § 38-99-10

- **Cybersecurity event:** an event resulting in unauthorized access to, disruption or misuse of, an information system or information stored on such information system.
  - **Safe Harbors.** It does not include:
    - The unauthorized acquisition of **encrypted** nonpublic information IF the encryption, process or key is not also acquired, released or used without authorization.
    - An event where the licensee has determined that nonpublic information accessed by an unauthorized person ***has not been used or released and has been returned or destroyed.***
  - **Information System:** a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial or process controls systems, telephone switching and private branch exchange systems, and environmental control systems.
- Note:**
- **Cybersecurity events under the law involve electronic records and systems only.**
  - **Unauthorized access to encrypted information is NOT a cybersecurity event.**
  - **A power outage or other benign cause of a disruption is not a cybersecurity event unless unauthorized access to NPI results.**



## **KEY DEFINITION | Information Security Program | § 38-99-10(7)**

- **‘Information security program’ means the administrative, technical, and physical safeguards that a licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle nonpublic information.**
- **This language is substantially similar to the requirements of the GLBA.**



# QUESTION: Am I exempt Under the Act?

**Section 38-99-70 sets forth exemptions for compliance with the **information security program** component of the Act.**

Licensees with less than 10 employees

Licensees covered by the information security program of another licensee

Licensees subject to HIPAA that submit written certification of compliance with HIPAA

Licensees that certify compliance with the New York Cyber Security Regulation and pertinent provisions of the SC Insurance Data Security Act including prompt investigation and cybersecurity event notification

➤ **Note: If a licensee ceases to qualify for an exception (exemption), the licensee has 180 days to come into compliance with the law.**



# QUESTION: What does being *exempt* mean?

Exemption	Exempt From	Still Required
Fewer than 10 employees	<ul style="list-style-type: none"><li>• Formal Information Security Program (Section 38-99-20)<ul style="list-style-type: none"><li>• Risk Assessment</li><li>• Risk Management</li><li>• Board Oversight</li><li>• Oversight of TPSP</li><li>• Program Adjustments</li><li>• Incident Response Plans</li><li>• Annual Certifications</li></ul></li></ul>	<p>Compliance with other provisions such as:</p> <ul style="list-style-type: none"><li>• Investigation of Cybersecurity Event</li><li>• Notices of Cybersecurity Events to the Director</li></ul>
Licensee covered by the Cybersecurity Program of Another Licensee	<ul style="list-style-type: none"><li>• Formal Information Security Program (Section 38-99-20)<ul style="list-style-type: none"><li>• Risk Assessment</li><li>• Risk Management</li><li>• Board Oversight</li><li>• Oversight of TPSP</li><li>• Program Adjustments</li><li>• Incident Response Plans</li></ul></li></ul>	<p>Compliance with other provisions such as:</p> <ul style="list-style-type: none"><li>• Investigation of Cybersecurity Event</li><li>• Notices of Cybersecurity Events to the Director</li></ul>



**QUESTION: What does being exempt mean for licensees compliant with HIPAA and the NY Cybersecurity Regulation?**

<b>Exemption</b>	<b>Exempt from</b>	<b>Still Required</b>
<b>HIPAA compliant and files a certification that it is HIPAA compliant</b>	<ul style="list-style-type: none"><li>• <b>Establishing another formal Information Security Program (Section 38-99-20)</b></li></ul>	<b>Compliance with other provisions such as:</b> <ul style="list-style-type: none"><li>• <b>Investigation of Cybersecurity Event</b></li><li>• <b>Notices of Cybersecurity Events to the Director</b></li><li>• <b>Annual certification that insurer is still HIPAA compliant</b></li></ul>
<b>Compliant with New York Cybersecurity Regulation and files a certification that that effect</b>	<ul style="list-style-type: none"><li>• <b>Establishing another formal Information Security Program (Section 38-99-20)</b></li></ul>	<b>Compliance with other provisions such as:</b> <ul style="list-style-type: none"><li>• <b>Prompt Investigation of Cybersecurity Event</b></li><li>• <b>Notices of Cybersecurity Events to the Director consistent with SC law</b></li><li>• <b>Annual certification that insurer is still compliant with New York Cybersecurity Regulation and with the investigation and</b></li></ul>



**QUESTION: Why does the Department plan to recognize an exemption for licensees who certify they are compliant with the New York Cybersecurity Regulation?**

<b>Requirement</b>	<b>SC Insurance Data Security Act</b>	<b>New York Cybersecurity Regulation</b>
<b>Cyber Security Event Reporting</b>	Notice must be provided within 72 hours from determination that a cybersecurity event has occurred; 13 categories of information must be included in the notice	<b>Notice must be provided within 72 hours of the determination that a cybersecurity event has occurred; but no detail as to information to be included in the notice to the Director.</b>
<b>Definition of Cyber security event</b>	Cyber security event does not include unauthorized acquisition of encrypted information	<b>The New York regulation does not include the SC Act's language</b>
<b>Investigation of a Cyber Security Event</b>	Licensee has an affirmative obligation to conduct a prompt investigation under the Act. Records must be maintained for five years and produced upon demand of the Director or his designee.	<b>No specific requirements regarding the prompt investigation of a cybersecurity event.</b>



# **The Act Does Not Apply to...**

- **Licensees that do not have an information system as that term is defined by the Act (i.e., the licensee has no electronic information).**
- **Licensees that do not have NPI.**
- **Licensees that only have the NPI of its parent or its affiliates.**
- **Risk retention groups chartered in other states.**
- **Assuming insurers chartered in other states**



***Qualifying for an exemption under the S.C. Insurance Data Security Act **does not exempt** a licensee from protecting PII, PHI or NPI under other state and federal laws such as:***

Law	Information Protected	Penalties
<b>Gramm Leach Bliley Act</b>	<ul style="list-style-type: none"> <li>• Nonpublic financial information including name, address, telephone combined with SSN, DL#, Account number, credit or debit card number, PINs</li> </ul>	Civil monetary penalties; fines and imprisonment for individuals who secure info through fraudulent means. Institution: \$100,000 for each violation; Officers and Directors \$10,000 each violation
<b>Fair Credit Reporting Act/Fair and Accurate Credit Transactions Act</b>	<ul style="list-style-type: none"> <li>• Credit information; businesses cannot publish more than five digits of a payment card number</li> <li>• Businesses that use this information must properly dispose of it</li> </ul>	Civil monetary penalties for violation of orders, \$40,000; violation of the duty to correct and update information, \$3756 per violation.
<b>Federal Trade Commission Act</b>	<ul style="list-style-type: none"> <li>• Failure to comply with privacy policies</li> <li>• Failure to provide reasonable and appropriate protection for sensitive consumer information</li> </ul>	Injunctions; restitution for consumers; repayment for investigation and prosecution costs; Civil penalties: \$40,000 per violation
<b>HIPAA</b>	<ul style="list-style-type: none"> <li>• Protected health information</li> </ul>	Penalties based on different categories and range from a minimum fine of \$100 to \$50,000 per record or violation; max: \$1.5M



# **Major Components of the Law**



**Risk Assessment**

**Establishment and Monitoring of an Information Security Program**

**Risk Management, Training & Due Diligence**


**Investigation of Cybersecurity Event(s)**

**Notification of Cybersecurity Event(s)**

**Reporting, Notices & Certification of Compliance**



# **Question: What does the law require of SCDOI Licensees who do not qualify for an exemption?**



<b>Risk Assessment and Implementation of Information Security Program</b>	<ul style="list-style-type: none"><li>• Conduct a risk assessment</li><li>• Based on risk assessment, implement an information security program</li></ul>
<b>Information Security Program Management and Maintenance</b>	<ul style="list-style-type: none"><li>• Designate an employee or vendor to be responsible for the information security program.</li><li>• Implement security measures appropriate for the size and complexity of the business</li></ul>
<b>Training &amp; Due Diligence</b>	<ul style="list-style-type: none"><li>• Provide cybersecurity awareness training for employees and third party vendors</li><li>• Exercise due diligence with the selection of third party vendors and require them to implement the necessary security measures.</li></ul>
<b>Incident (Cybersecurity Event) Response &amp; Notification</b>	<ul style="list-style-type: none"><li>• Implement an incident response plan.</li><li>• Notify the Director or his designee of cybersecurity events.</li><li>• Notify the producer of record of cybersecurity events</li></ul>



# What does the law require of SCDOL Licensees?

## (continued)



### Reporting

- Executive management must report to its Board of Directors (if one exists) in writing at least annually on the overall status of its information security program and other material matters.

### Insurer Certification

**Due by**  
**February 15, 2020**

- Domestic *insurers* must certify compliance with the information security program requirements of the law annually.
- If there are areas where material improvement is needed, this must be documented and the remedial efforts to correct the deficiency described.
- Documentation must be retained for five years

### Board Responsibilities

- Oversee the development, implementation and maintenance of the Information Security Program
- May Delegate responsibilities to management or other for implementation but Board is responsible for oversight



**July 1, 2019**

- **Information Security Program**

**July 1, 2020**

- **Third-Party Service Provider Program**

**Jan. 1, 2019**

- **Breach notification reports due**
- **Risk Assessments**
- **Policies and Procedures**
- **Info Sec Personnel**
- **Incident Response Plan**
- **Notification Procedures**

**Feb. 15, 2020**

- **Certification of Compliance Reports due**

## **South Carolina's Compliance Timeline**



# Data Protection Requirements Affecting Insurance Industry *before* SCIDSA

Requirement	HIPAA (1996) (PHI)	GLBA (1999) (PII)	FACTA/FTC Act
<b>Risk Assessment</b> 16 CFR § 314.4(b)	Yes. HIPAA Security rule requires covered entities to conduct a risk analysis to help covered entities identify the most effective and appropriate administrative, physical and technical safeguard to secure electronic PHI. See 45 CFR 164.302-318	Yes. GLBA requires companies to identify and assess the risks to customer information in each area of its operation and to evaluate the effectiveness of current standards in controlling these risks.	Yes. The Act does not specify security standards, but has exercised jurisdiction over data privacy and has taken the position that inadequate data security is a deceptive business practice. See <i>In the Matter of BJ's Wholesale Club, Inc.</i> , 140 FTC 465 (FTC Consent Order, Sept. 20, 2005).
<b>Information Security Program</b> 16 CFR § 314.3	Yes. Covered entities are required to implement data protection policies and safeguard including technical safeguards, which include automated processes designed to protect data and control access, such as using authentication controls and encryption technology	Yes. ISP must be appropriate for the company's size and complexity, the nature and scope of its activities and the sensitivity of the information it handles	<p>FTC also requires reasonable security be provided for certain data based on:</p> <ul style="list-style-type: none"> <li>• the data's sensitivity;</li> <li>• the nature of the company's business operations;</li> <li>• the types of a risks a company faces; and</li> <li>• reasonable protections that are available.</li> </ul> <p>Retain data for only the time necessary to fulfill a legitimate business or law enforcement need.</p>



# Data Protection Requirements Affecting Insurance Industry *before* SCIDSA

Requirement	HIPAA (1996) (PHI)	GLBA (1999) (PII)
Third Party Service Providers 16 CFR Section §314.4(d)	Yes. HIPAA applies to business associates as well.	Select service providers that are able to maintain appropriate safeguards, contractually require service providers to maintain safeguards, and oversee service providers' handling of customer information
Employee Training 16 CFR § 314.4(b)(1)	Employees must be trained	Yes.
Investigation 16 CFR §314.4(b)(3)	Yes.	Yes.
Notifications Interagency Guidance issued by the FTC and Federal Financial Institutions Examinations Council (FFEIC).	HHS also requires covered entities to notify individuals when their unsecured PHI has been breached	OCC and FRB requires financial institutions to notify the regulator, affected customers, etc., when there has been unauthorized access to sensitive information.
Designate employees to implement ISP 16 CFR § 314.4(a)	Covered entities are required to assign responsibility to the ISP to appropriate individuals	Yes.



The background of the slide is a light blue and white graphic. It features a central, stylized padlock icon with a keyhole, rendered in a light blue color. Surrounding the padlock are various circuit-like patterns, including lines and circles, in shades of blue and white, giving it a technological or digital feel.

# ***Determining Compliance with the South Carolina Insurance Data Security Act***



# **SCDOI INVESTIGATIONS/EXAMINATIONS | § 38-99-50**



**Under Section 38-99-50, the Director has the authority to examine and investigate a licensee to determine whether a violation of the Act has occurred. This authority is in addition to any other examination or investigation authority that he possesses under the law.**

## **Investigations**

**Investigations of allegations that a licensee has violated the law will be conducted under this section and the director's other general investigative authority in Title 38.**

## **Examinations**

**Examinations may be conducted on a full scope or targeted basis in accordance with the NAIC guidelines and the NAIC IT Questionnaire and any supplemental guidance.**



# COMPLIANCE TIPS

**These next presentation slides are designed to provide some guidance to help you comply with the Act. The intent is to provide some general insight into what South Carolina regulators may look for as a part of any investigation to determine compliance with the Act. We hope this information will inform the development of your Information Security Program (ISP). Document your compliance efforts.**

## **Tip:**

- **Be methodical in your approach to compliance.**
- **Assign responsibilities for the ISP and hold people accountable.**
- **Devote the necessary time and resources to your risk assessment.**
- **Develop a plan/framework for your information security program with checklist(s) for each significant part of the Act.**
- **Develop security policies, standards and guidelines based on your business' risk assessment.**
- **Train your employees.**



## **Determining Compliance: Regulatory Considerations**

### **Does the Act Apply to the Licensee?**

- **Does the licensee operate, maintain, utilize or control any electronic system for the collection, processing, sharing or storing electronic information?**
- **Does the licensee possess or collect nonpublic information?**
  - **Would unauthorized disclosure result in a material adverse impact to operations, profitability, or security?**
  - **Does the NPI consist of an individual's name, number and other unique identifiers?**
  - **Does the nonpublic information consist of information obtained from a healthcare provider?**
- **If the licensee does not have an information system, the Act does not apply.**
- **If the licensee has an information system and the answer to one of more of the questions about nonpublic information is yes, the Act applies unless the licensee qualifies for an exemption.**



# **Determining Compliance: Regulatory Considerations**

**Does the licensee have an information system and collect NPI?**

**Yes**

- **Is there an IT management structure?**
- **Who is accountable for implementation of the ISP?**
- **What role does the Board or senior management play with ISP governance?**

**No**

- **Is the licensee exempt?**
- **If so, which exemption applies?**



# **Determining Compliance: Regulatory Considerations**

## **Has the Licensee Assessed the Company's Risk?**

**1**

- **Identified reasonably foreseeable internal and external threats to NPI**

**2**

- **Assessed the likelihood and potential damage from these threats**

**3**

- **Assessed sufficiency of policies, procedures and information systems and other safeguards to manage these threats**

**4**

- **Implemented information safeguards to manage threats, and at least annually, assessed the effectiveness of the safeguards**

**5**

- **Included cybersecurity risks in the enterprise risk management process**



# **Determining Compliance: Regulatory Considerations**

## **Is the ISP appropriate for the licensee's size and complexity?**

- **How large is the licensee's business? How many employees?**

- **10 or more employees?**
- **Less than 10 employees?**

- **Does the licensee collect, store, distribute NPI?**

- **Has that data been classified?**
- **What laws govern the data collected by the licensee?**

- **Does the program include the basic elements of the South Carolina Insurance Data Security Act?**

- **Is there more than one ISP? If so, are the programs coordinated?**
- **Is encryption software on any of the systems?**



# Determining Compliance: Regulatory Consideration

**Based on the licensee's risk assessment, does the ISP address these basic elements?**

## Technology



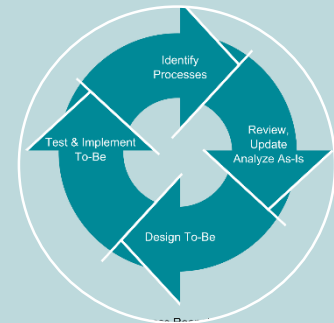
- System security
- Firewalls
- Intrusion Detection and Prevention
- Physical security
- Vulnerability Assessment
- Penetration Testing
- Application Security

## People



- Training
- Awareness
- HR Policies
- Roles and Responsibilities
- Mobile Computing
- Social Engineering
- Acceptable Use
- Performance Management

## Process



- Risk Management
- Asset Management
- Data Classification
- Access Management
- Incident Management
- Incident Response



# **Determining Compliance: Regulatory Considerations**

## **What training does licensee provide its employees?**

### **Training Should Include These Basic Concepts**

**Each employee is responsible for protecting the licensee's data**



**Safeguarding computers by locking them or keeping them in a secure place.**

**Employees should be familiar with the laws that protect the information they use to perform their jobs.**

**Employees are responsible for notifying management of suspicious computer activity**

**Employees should be taught to recognize email scams and not respond to emails they do not recognize.**



## **Determining Compliance: Regulatory Considerations**

### **Has the Licensee implemented risk management or risk mitigation policies and procedures?**

**Is there a hardware, software and information system inventory?**

**Is there a disaster recovery plan or analysis on how the short-term unavailability of data will impact operations?**

**Are there updated and test data back ups, recovery and contingency procedures?**

**Does password access correspond with the employee's job description and the principle of least privilege?**

**Are there detailed password guidelines and periodic password change protocols?**

**Is there virus scanning software installed on all relevant devices on- and off-site so licensee is informed of threats?**

**Does the licensee conduct phishing campaigns to test the susceptibility of its employees to phishing campaigns?**



## **Determining Compliance: Regulatory Considerations**

### **Has the Licensee implemented risk management or risk mitigation policies and procedures?**

**Has the licensee reviewed offsite access to computer networks and usage of storage media?**

**Has the licensee created forms to document investigation, mitigation, and resolution of security incidents?**

**Has the licensee trained its employees? Do employees know that they are subject to administrative monitoring?**

**Has licensee documented the procedures for reporting and documenting security incidents?**

**Does licensee have an audit log of excessive or unusual activity?**

**Does licensee require all lost or stolen access devices such as key card, keys, mobile phones or mobile devices be reported?**



# Third Party Service Provider Program

Section 38-99-20(F) | **Due:** July 1, 2020

## Third party service provider is

*a person not otherwise defined as a licensee that contracts with a licensee to maintain, process, store or otherwise is permitted access to nonpublic information through its provision of services to the licensee. See Section 38-99-10(16).*

- **Licensees must implement a third-party service provider program by July 1, 2020.**
- ***Licensees must also:***
  - **Exercise due diligence in selecting its third party service provider.**
  - **Require a third party service provider to implement appropriate administrative, technical and physical measures to protect and secure information systems and NPI held by the service provider.**



## **Determining Compliance: Regulatory Considerations**

**Does licensee have a third party service provider program?**

**Is there a third party service provider security policy?**

- Is the policy based on the Licensee's risk assessment?
- Can the TPSP provide your data the same protection you are required to provide?

**TPSP Policy should address**

- Has there been an assessment of risk posed by the TPSP?
- What security practices must the TPSP meet?
- Are there periodic assessments of the TPSP?

**What does the contract say?**

- Is there a written agreement that sets forth the terms of the engagement and what the TPSP can do with the information?
- Is there any auditing or oversight of the TPSP's activities?



# **Determining Compliance: Regulatory Consideration**

**Is there evidence that licensee exercised due diligence when selecting the TPSP?**

## **Reputation of the TPSP**

- How long has it been in business?
- What qualifications does the TPSP have?
- What relationships does the TPSP have with other vendors?

## **Access to Sensitive Information**

- Does the TPSP have access to information systems?
- What safeguards are in place to protect licensee's data?
- Who has access to the TPSP's information systems?

## **Contractual Terms**

- What does your contract say about data security?
- Is there a gap between your legal obligations and the vendor's systems?
- What happens if there is a cybersecurity event involving the TPSP's systems?

## **Insurance**

- Does the licensee have cyber insurance?
- Does the TPSP have cyber insurance?
- What other risk mitigation policies or procedures does the licensee have in place?



# **Are licensee's information security policies documented?**

## ***Examples of Key Information Security Program Policy and Procedures Documentation***

- ☐ **Information Security Governance?**
- ☐ **Risk Management?**
- ☐ **Compliance?**
- ☐ **Incident Management?**
- ☐ **Security Operations?**
- ☐ **Vulnerability Management?**
- ☐ **Acceptable Use?**
- ☐ **Identity Management?**
- ☐ **Security Architecture?**
- ☐ **Network Security?**
- ☐ **Application Security?**
- ☐ **Business Continuity?**
- ☐ **Security Program Management?**
- ☐ **Security Operations?**
- ☐ **Management?**
- ☐ **Risk Management?**
- ☐ **Vulnerability Management?**
- ☐ **Incident Management?**
- ☐ **Security Policy Management?**
- ☐ **Compliance Management?**
- ☐ **Training and Awareness?**



## **COMPLIANCE INSIGHT**

### ***COMMON INFORMATION SECURITY PROGRAM MISTAKES***

- **Not developing or failing to implement policies and procedures**
- **Not allocating sufficient resources to support ongoing processes and procedures**
- **Not enforcing policies and procedures**
- **Not designating specific groups to implement and maintain the program and holding them accountable**
- **Failing to effectively manage **third party** access to PII, NPI or PHI**
- **Failing to adequately train or monitor employee(s)**



# **SCDOI INVESTIGATION CHECKLIST**

## **KEY COMPLIANCE DOCUMENTATION EXAMPLES**

- ☐ **Privacy Policy**
- ☐ **Risk Assessment Report**
- ☐ **Annual Assessment/Annual Reports**
- ☐ **Information Security Policy and Procedures**
- ☐ **Incident Response Policy and Procedures**
- ☐ **Reports on Cybersecurity Incident Investigations**
- ☐ **Certification of Compliance Forms**
- ☐ **Cyber incident logs**
- ☐ **Third Party Service Provider Policies and Procedures**
- ☐ **Third Party Service Provider Agreements**
- ☐ **Training Materials**
- ☐ **Annual Report to the Board or Senior Management**



# **Determining Compliance: Regulatory Considerations**

## **Does the licensee have an incident response plan?**

**Incident Response Plans** are required as a part of the licensee's information security program. Incident Response Plans must include:

- ☐ **The internal process for responding to a cybersecurity event**
- ☐ **Clearly defined roles and responsibilities for employees and identify who has decision making authority**
- ☐ **A list of third party resources (IT specialists, law firms)**
- ☐ **A communication plan for press releases (templates, scripts and a designated person for media calls)**
- ☐ **Immediate remedial steps to be take to mitigate damage**
- ☐ **Documentation and reporting regarding cybersecurity events**



## **Determining Compliance: Regulatory Considerations**

**Did the Licensee respond timely to an cybersecurity event?**

# **Stages of Incident Response**

**Verification  
And Notice to  
the Director**

**Containment  
and  
Mitigation**

**Investigation  
and Analysis**

**Notification**

**Post-  
Response  
Process  
Review**

- **Licensees should keep a record of actions taken responding to an incident.**
- **Evidence related to the cybersecurity event should be preserved.**



# Determining Compliance: Regulatory Considerations

## What actions did the licensee take to verify the cybersecurity incident?

Did the licensee:

- ☐ Identify the affected systems or hardware?
- ☐ Determine the nature of the data maintained on those systems or hardware?
- ☐ Determine the type of incident. Was the disclosure:
  - ☐ Internal or external?
  - ☐ Caused by an employee or third party service provider?
  - ☐ The result of a malicious attack?
- ☐ Determine whether the incident exposed or is reasonably likely to expose NPI? If so, was the data on the system encrypted?
- ☐ Determine whether PII was affected and the data elements that are at risk?

Once unauthorized access, misuse or disruption has been verified, provide an initial notification to the Director or his designee.



# **Determining Regulatory Compliance**

## **What did licensee do to contain and mitigate the Cybersecurity Event?**

- ☐ **Did licensee contain the threat by:**
  - ☐ **Blocking accounts, websites and services?**
  - ☐ **Restricting internet connectivity or suspend internet access?**
  - ☐ **Changing passwords?**
  - ☐ **Isolating the computers by disconnecting them?**
- ☐ **Did the licensee reduce the impact of the event by:**
  - ☐ **Having other systems operate in a manual mode?**
  - ☐ **Creating alternate accounts?**
- ☐ **Did the licensee eradicate the threat by:**
  - ☐ **Removing the malware and patched vulnerabilities?**
  - ☐ **Deleting fake user names, reset passwords and installed two-factor authentication?**



# **Determining Compliance: Regulatory Considerations**

## **Did licensee initiate a prompt investigation?**



**Collect data including information about the cybersecurity event:**

- How the cybersecurity event was discovered?**
- What is the nature of the cybersecurity event?**
- When did it first occur? Is it ongoing?**
- How long did the cybersecurity event last? Where did it occur?**
- What was the method of system intrusion?**
- Are systems and files compromised?**
- What NPI was exfiltrated?**



# **Determining Compliance: Regulatory Considerations**

## **What are the legal implications of the cyber event?**

**Licensees should consider the following:**

- **Did the cybersecurity event trigger individual, regulatory consumer or media notifications?**
  - **If so, identify the jurisdictions where any affected persons may reside to assess which state laws may be triggered.**
  - **Identify whether the type of data triggers additional statutory obligations under the law.**
    - **Is the data subject to HIPAA, GLBA, FCRA, FTC, FACTA?**
  - **Review all relevant contracts and policies**
- **Review with your attorney notice requirements and plans for communicating with the media, regulators, etc.**
- **If notifications are necessary, prepare a notification plan.**



# **NOTIFICATION REQUIREMENTS | Reinsurers | § 38-99-40(E)**

<b>Reinsurer Type</b>	<b>Notification Requirements</b>
<b>Assuming Reinsurer with no consumer relationship</b>	<b>Notify the affected ceding insurers and the Director within 72 hours</b>
<b>Assuming insurers with consumer relationship</b>	<b>Notify consumers pursuant to Section 39-1-90</b>
<b>Assuming Insurers when a cybersecurity event involves a third party service provider</b>	<b>Notify ceding insurers and Director within 72 hours of receiving notice from the third party service provider</b>
<b>Ceding insurers with a consumer relationship</b>	<b>Notify consumers pursuant to Section 39-1-90</b>
<b>Notice to the Producer of Record</b>	<b>If cybersecurity event is with an insurer or third party service provider and a consumer accessed services through an independent producer, insurer must notify the producers of record of all consumers as soon as practicable</b>



# Notification Requirements | SCIDSA | NPI and PHI

**Section 39-1-90 requires notification if 1) data was unsecured (not encrypted); 2) data was acquired by an unauthorized person; 3) illegal use of the information has occurred or is likely to occur; or 4) use of the information creates a material risk of harm to a South Carolina resident.**

Code Section	Notify	Notice to State Agency/Timing	Affected Individual Threshold	Content of the Notice
<b>S. C. Code Section 39-1-90</b>	<ul style="list-style-type: none"><li>• <b>Affected residents</b></li><li>• <b>SC Department of Consumer Affairs, Consumer Protection Division</b></li><li>• <b>Credit Reporting Agencies</b></li></ul>	<b>Without unreasonable delay (notice must be delayed if law enforcement thinks notice will impede its investigation)</b>	<b>1,000</b>	<b>Notice must include information on timing, distribution and content of notice to individuals</b>



# **Federal Notification Requirements** | **Protected Health Information**

<b>Code Section</b>	<b>Notify</b>	<b>Timing</b>	<b>Affected Individual Threshold</b>	<b>Content of the Notice</b>
<b>45 CFR Section 164.402</b>	<ul style="list-style-type: none"><li>• <b>Affected individuals (within 60 days' discovery)</b></li><li>• <b>Media notification (within 60 days' discovery of the breach)</b></li><li>• <b>HHS must be notified concurrently with notice to individuals</b></li></ul>	<b>Not later than 60 days from discovery</b>	<b>500</b>	<ul style="list-style-type: none"><li>• <b>Description of what happened</b></li><li>• <b>Description of the type of information impacted</b></li><li>• <b>Steps individuals should take to protect themselves</b></li><li>• <b>Description of what the company is doing to investigate, mitigate, and protect against further breaches</b></li><li>• <b>Contact procedures for individuals to ask questions</b></li></ul>



# **Federal Notification Requirements | GLBA**

**GLBA does not specify any notice requirements. However, if a data breach occurs, the FTC recommends that an organization:**

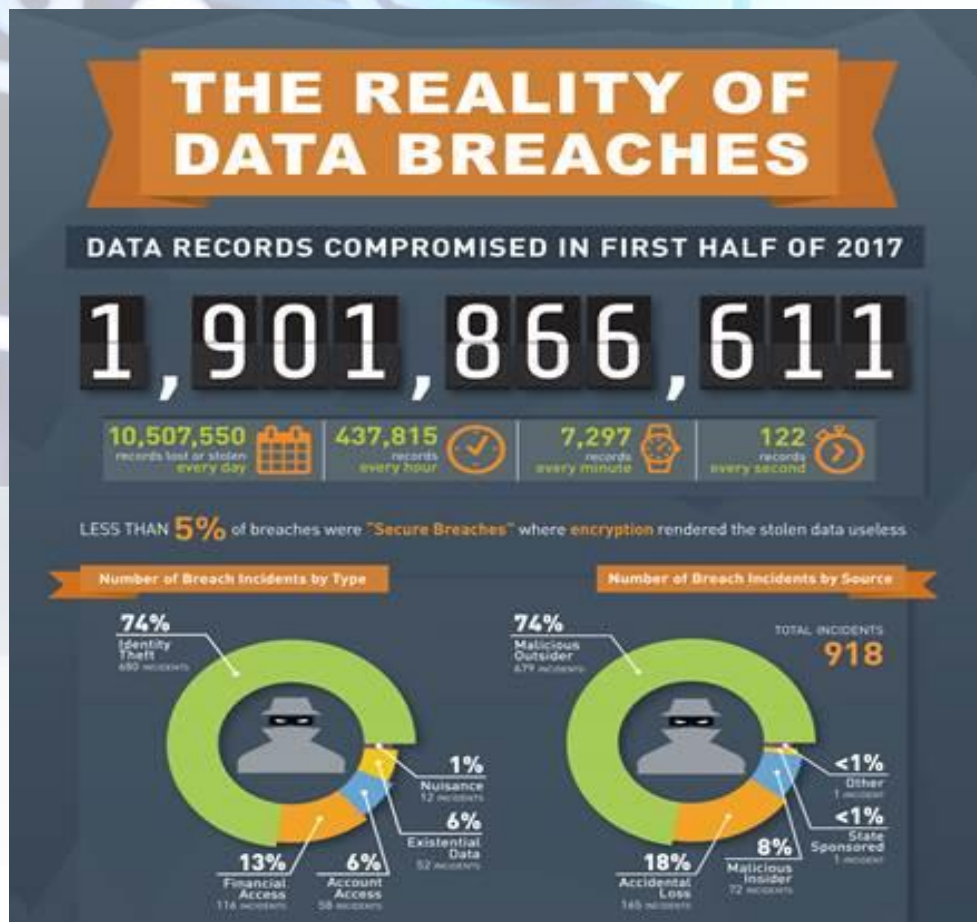
- ☐ Take immediate action to secure any information that has been compromised**
- ☐ Preserve relevant information and investigate how the breach occurred**
- ☐ Employ security professional(s) to help assess the breach as soon as possible**
- ☐ Consider notifying consumers or businesses affected by the breach, the credit bureaus and law enforcement.**



# THE COSTS OF NONCOMPLIANCE

Section 38-99-80 provides:

*A licensee who violates a provision of this chapter is subject to penalties as provided in Section 38-2-10.*



Licensee Type	Negligent Violation	Intentional Violation
Company Licensee	Up to \$15,000 per violation or suspension or revocation (or combination thereof)	Up to \$30,000 per violation or suspension or revocation (or combination thereof)
Individual Licensee	Up to \$2,500 per violation or suspension or revocation of license (or combination thereof)	Up to \$5,000 per violation or suspension or revocation of license (or combination thereof)

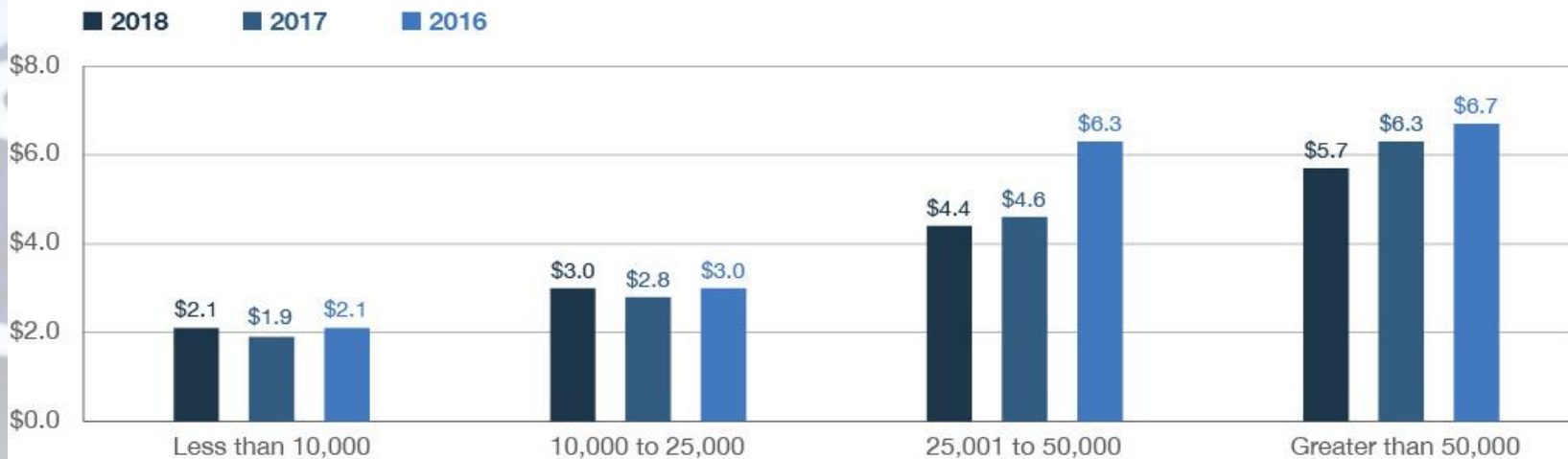


# Noncompliance: Pay now or pay later

## 2018 Data Breach Costs

Average total cost by size of the data breach

Measured in US\$ millions



**For FY 2018, the average total cost of a data breach, the average cost for each lost or stolen record (per capita cost), ranges:**

- **\$2.2 million for incidents with fewer than 10,000 records to \$6.9 million for more than 50,000 records**
- **Mega breaches (1 million records) could cost as much as \$39.49 million**



# COMPLIANCE TIPS

**We hope this information will inform the development of your Information Security Program (ISP). Document your compliance efforts.**

## **Tip:**

- **Be methodical in your approach to compliance.**
- **Assign responsibilities for the ISP and hold people accountable.**
- **Devote the necessary time and resources to your risk assessment.**
- **Develop a plan/framework for your information security program with checklist(s) for each significant part of the Act.**
- **Develop security policies, standards and guidelines based on your business' risk assessment.**
- **Train your employees.**









**Reporting Obligations Under the Act**



# **Submit Annual Report to Board | § 38-99-20(E)**

## **Board Report must include information on:**

- **Overall status of the information security program and the licensee's compliance with the law**
- **Material matters related to the information security program such as:**
  - **Risk assessment**
  - **Risk management control decisions**
  - **Third party service provider arrangements**
  - **Results of testing**
  - **Cybersecurity events or violations and management's response**
  - **Recommendations for changes in the information security program**

**The Act does not require the licensee to prepare a report if there is no board. However, preparing a report for senior management may be advisable.**



# **Reporting Obligations Under the Act**


## **Compliance Certification | §§ 38-99-20(I)**

### **Due Annually:**

- **Each insurer domiciled in this state must submit to the Director, a written statement by February 15, certifying that the insurer is in compliance with the requirement set forth in 38-99-20(I) of this Act.**
- **Each insurer shall maintain for examination by the Department of all records, schedules and data supporting this certificate for a period of five years.**
- **To the extent an insurer has identified areas, systems or processes that require material improvement, updating or redesign, the insurer shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes.**




# Report Submissions through the SCDOI Cybersecurity Portal

**SOUTH CAROLINA**  
DEPARTMENT OF INSURANCE

[f](#) [t](#) [y](#) [v](#) [r](#) [e](#) [s](#)

CONSUMERS   LICENSING & CE   INSURERS   CAPTIVES   ABOUT US   HOW DO I...?

Search... 

[Feature Links](#) > [Cybersecurity](#)

**Cybersecurity**

On May 3, 2018, Governor Henry McMaster signed into law the [South Carolina Insurance Data Security Act](#) (the "Act"). The Act will become effective on January 1, 2019. South Carolina is the first state in the nation to pass this important and timely legislation which is modeled after the NAIC Insurance Data Security Model Law.

The Act is codified in Title 38, Chapter 99 of the South Carolina Code of Laws. The Act defines the requirements applicable to a "licensee" and establishes standards for data security and standards for the investigation of and notification to the Director of a cybersecurity event.

### Key Implementation Dates

**January 1, 2019:** South Carolina Insurance Data Security Act becomes effective. This requires, among other things, that a licensee notify the Director no later than 72 hours after determining that a cybersecurity event has occurred when certain criteria are met.

**July 1, 2019:** Licensees must have implemented Section 38-99-20 by this date. This section requires that licensees establish a comprehensive, written information security program by July 1, 2019.

**July 1, 2020:** Licensees must have implemented Section 38-99-20(F) by this date. This section details additional requirements for licensees who contract with third-party service providers that maintain, process, store or otherwise is permitted access to nonpublic information through its provision of services to the licensee.

**February 15, 2020:** Beginning on this date, each insurer domiciled in South Carolina must annually submit to the Director a written statement certifying that the insurer is in compliance with the requirements set forth in Section 38-99-20.


### Additional Information


The Department will issue a series of bulletins regarding the implementation of this legislation and each will be copied below as they become available.


1. [Bulletin 2018-02. South Carolina Insurance Data Security Act](#). This bulletin provides answers to questions such as to whom does the Act apply, what does the legislation do, and when will the legislation be effective.
2. [Bulletin 2018-09. Cybersecurity Event Reporting Form](#). This bulletin addresses the process for reporting a cybersecurity event and provides guidance regarding what constitutes a cybersecurity event.


View a copy of the ["Report a Cybersecurity Event" form](#).


[File a Complaint](#)  
[SC DOI Connect Login](#)  
[Investigating Fraud](#)  
[SC Safe Home](#)  
[Search SCDOI Database](#)  
[Government and Industry Resources](#)  
[Employment at the DOI](#)  
[Report State Agency Fraud](#)  
[Cybersecurity](#)

 **ONLINE FORMS**

 **BULLETINS & ORDERS**

 **ONLINE SERVICES**

 **MARKET ASSISTANCE**

 **NOTIFICATION SUBSCRIPTIONS**




## **Provide Notice of a Cybersecurity Event | §38-99-40**

**Each licensee shall notify the Director within 72 hours of a determination that a cybersecurity event has occurred IF**

- ☐ **South Carolina is the state of domicile for an insurer or the home state of a producer**
- ☐ **Nonpublic information of 250 or more South Carolina consumers is involved and either**
  - ☐ **Notice is required to be provided to a governmental or self-regulatory agency or any other supervisory body pursuant to state or federal law or**
  - ☐ **The cybersecurity event has a reasonable likelihood of materially harming:**
    - ☐ **Any consumer residing in this state;**
    - ☐ **Any material part of the normal operations of the licensee**
- ☐ **Insurers must also notify the producer of record of a cyber security event.**




# SCDOI Online Reporting Form | Section 1

**SOUTH CAROLINA**  
DEPARTMENT OF INSURANCE

Home | [SCDOI Online Services](#) | [Search SCDOI Database](#) | [Contact Us](#)SCDOI Online Services

[SCDOI Connect Login](#)

**South Carolina Department of Insurance**  
Street Address: 1201 Main Street, Suite 1000, Columbia, S.C. 29201  
Mailing Address: P.O. Box 100105, Columbia, S.C. 29202-3105  
Telephone: (803) 737-6160 or 1 (800) 768-9999  
Fax: (803) 737-6231 | Email: [datasecurity@doi.sc.gov](mailto:datasecurity@doi.sc.gov)

**REPORT A CYBERSECURITY EVENT**

[Under the South Carolina Insurance Data Security Act, licensees are required to report Cybersecurity Events to the S.C. Department of Insurance in accordance with the requirements of Section 38-99-40.](#)

**Section 1. Information of Entity Experiencing Cybersecurity Event**

Licensee Type

NAIC Code	NPN #	SBS #	FEIN Code
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Name	<input type="text"/>		
Address 1	<input type="text"/>		
Address 2	<input type="text"/>		
Suite/Apt/Building	<input type="text"/>		
City, State, Zip	<input type="text"/>	<input type="text"/>	<input type="text"/>
Telephone	<input type="text"/>		
Fax	<input type="text"/>		
Email Address	<input type="text"/>		



# SCDOI Online Reporting Form | Sections 2, 3 and 4

## Section 2. Event Dates

Estimated Occurrence

☐ Unknown

Estimated End

☐ Unknown

Date Discovered

## Section 3. Event Type (Check all that apply)

☐ Data Theft by Employee/ Contractor

☐ Hackers/ Unauthorized Access

☐ Lost During Move

☐ Phishing

☐ Improperly Released/ Exposed/ Displayed

☐ Stolen Laptop(s)

☐ Computer and Equipment

☐ Improperly Disposed

☐ Other

## Section 4. Circumstances Surrounding the Cybersecurity Event

How was the information exposed, lost, stolen, or accessed? Include the identity of the source of the Cybersecurity Event, if known.

How was the Cybersecurity Event discovered?

What actions are being taken to recover lost, stolen or improperly accessed information?



# SCDOI Online Reporting Form | Section 5

## Section 5. Third-Party Involvement

Did the Cybersecurity Event occur within the information / systems maintained by the licensed entity or individual reporting the Cybersecurity Event or within the information / systems maintained by a third-party service provider? Our Information / Systems ▼

Name of the Third-Party Service Provider

Description of the Third-Party Service Provider

What were the specific roles and responsibilities of the Third-Party Service Provider?



# SCDOI Online Reporting Form | Section 6

## Section 6. Information Involved (Check all that apply)

### ☒ Demographic Information

☐ Name

☐ Date of Birth

☐ Address

☐ Mother's Maiden Name

☐ Driver's License

☐ SSN

☐ Passport

☐ Other

### ☒ Health Information

☐ Medical Records

☐ Lab Results

☐ Medications

☐ Treatment Information

☐ Physician's Notes

☐ Other

### ☒ Financial Information

☐ Bank Account Information

☐ Credit Card

☐ Debit Card

☐ Other

### ☒ Other

Was the electronic information involved in the Cybersecurity Event protected in some manner? ☐ Yes ☐ No ☐ N/A It involved paper records only

Describe the efforts being undertaken to remediate the situation which permitted the Cybersecurity Event to occur



# SCDOI Online Reporting Form | Sections 7, 8 and 9

## Section 7. Number of Individuals / Entities Affected

Number affected nationally	<input type="text"/>	<input type="checkbox"/> Unknown
Number affected in South Carolina	<input type="text"/>	<input type="checkbox"/> Unknown

## Section 8. Business-Related Information

If the licensee's own business data was involved, please provide details about the type(s) of data involved

## Section 9. Notification Requirements

Is a notice to impacted South Carolina residents / entities required under South Carolina or federal law? ☒ Yes ☐ No ☐ Unknown

If yes, provide the date of notification: (Note: You should also upload a copy of the notice if not already provided to the SCDOI.)

<input type="text"/>	<input type="checkbox"/> Copy of notice will be sent on a subsequent date
----------------------	---



# SCDOI Online Reporting Form | Sections 10 and 11

## Section 10. Law Enforcement

Has a police report been filed? Has any regulatory, governmental, or other law enforcement agency been notified? (If yes, please attach documentation of report / notification unless already provided to the SCDOI.)

Police Report: ☒ Yes ☐ No ☐ Will be responding on a subsequent date

If yes, provide the date of notification

Regulatory Agency: ☒ Yes ☐ No ☐ Will be responding on a subsequent date

If yes, provide the date of notification

## Section 11. Contact Information of Individual Familiar with Cybersecurity Event and Authorized to Act on Behalf of the Licensee

First

Middle

Last

Title

Address 1

Address 2

Suite/Apt/Building

City, State, Zip

Telephone

Fax

Email Address



# SCDOI Online Reporting Form | Section 12

## Section 12. Attachments

Items to Attach:

1. A report of the results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed.
2. A copy of the licensee's privacy policy.
3. A statement outlining the steps the licensee will take to investigate and notify consumers affected by the Cybersecurity Event.

File	Document Type	Action
<a href="#">Click to select file</a>	Internal Review	
<a href="#">Click to select file</a>	Privacy Policy	
<a href="#">Click to select file</a>	Investigation Outline	

[Click to Add File\(s\)](#)

## Section 13. Attestation

I attest, to the best of my knowledge, that the information submitted on this form is true and correct to the best of my information and belief. By submitting this form, I am acknowledging that I am authorized to submit this form on behalf of the licensee or company. I further understand and agree that Section 38-99-60 of the South Carolina Code of Laws affords confidential treatment to certain information submitted to the SCDOI in accordance with Chapter 99. However, I understand that under state or federal law, the South Carolina Department of Insurance may be required to release statistical or aggregate information provided in this cybersecurity event notification. I acknowledge that copies of consumer notices may also be made available via the Department's website and the Department may also make available summary information related to cybersecurity events requiring public notification such as the identity of the licensee or third-party service provider, the number of individuals affected, the actions taken by the licensee to remedy the cybersecurity event and services available to consumers. I understand that Section 38-99-60 also gives the Director the authority to use the documents, materials or other information furnished by a licensee or someone acting on the licensee's behalf in furtherance of regulatory or legal actions brought as a part of the director's duties.

☐ Yes

[Submit Report](#)





# **FREQUENTLY ASKED QUESTIONS**

**About Implementation of the South Carolina Insurance Data  
Security Act**



**QUESTION:** *Is it the Licensee's responsibility to determine what is "necessary and appropriate" relative to "authorized individuals" under Section 38-99-10(1)?*

**Yes, this is the licensee's responsibility. The Licensee must make the determination that it is "necessary and appropriate" for any authorized individuals to have access to nonpublic information held by the licensee and its information systems.**



**QUESTION:**

***Under Section 38-99-20(A), the Act requires a Risk Assessment.  
Can this be a “self assessment” done in-house?  
Will licensees be required to use a third party vendor to  
conduct the assessment?***

**No, the Act does not require a licensee to use a third party vendor. There is nothing in the Act that precludes a licensee from conducting a self-assessment or from hiring a third party vendor to conduct the assessment. However, the assessment must be performed in accordance with the Act.**

**The Act provides that the licensee must make a determination based on the size and complexity of the Licensee how to effectively conduct a Risk Assessment that:**

- (1) Identifies reasonably foreseeable internal or external threats that could result in the unauthorized access to or transmission, disclosure, misuse, alteration, or destruction of nonpublic information including the security of information systems and nonpublic information that are accessible to or held by third-party service providers;**
- (2) Assesses the likelihood and potential damage of these threats, considering the sensitivity of the nonpublic information;**
- (3) Assesses the sufficiency of policies, procedures, information systems, and other safeguards in place to manage these threats, taking into consideration threats in each relevant area of the licensee’s operations... etc., and complies with the other sections of the Act**



**QUESTION:**      *Should a Licensee send supporting documentation along with the Certification of Compliance?*

**The licensee must submit the compliance certification to the Department but is not required to submit explanatory or additional materials with the certification. The certification is intended as a stand-alone document required by the statute. The Department also expects that the licensee will maintain the documents and records necessary to support the certification, should the Department request such information in the future.**



## **QUESTION:**

*Under the Section 38-90-70(A)(1), “a licensee with fewer than ten employees, including independent contractors;...” are exempt from the Data Security requirement? Does this provision mean ten employees in South Carolina or across the country?*

**This means that South Carolina licensees with fewer than ten employees within the entire company/business are exempt from the information security program requirements of the Section 38-99-20. The licensee must comply with other sections of the Act. The employees do not have to all be geographically located in South Carolina.**



**QUESTION:** *Do insurance companies licensed to do business in South Carolina, but domiciled in other states need to comply with the Act?*

**Yes. The Act defines a Licensee as “a person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State but does not include a purchasing group or a risk retention group chartered and licensed in a state other than this State or a licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction.”**

**Under that definition, insurance companies domiciled in other states that are doing business in S.C. (but that are not acting as a purchasing group or risk retention group chartered and licensed in another state, or as an assuming insurer domiciled in another state) are included in the definition of Licensee.**



**Question: What information will licensees be required to retain under Section 38-99-20(B) (4)? How long must licensees retain this information?**

**Section 38-99-20 (B)(4) addresses retention schedules. The Act requires licensees to develop a schedule for retention of nonpublic information and a mechanism for destruction of nonpublic information when no longer needed. A retention schedule is a document listing the business' records, the length of time each document will be retained as an active record, the reason for its retention (administrative, legal, fiscal or historical) and the disposition of those records.**

**This provision does not require licensee to retain nonpublic records, but instead ensures that licensees who store nonpublic information do not retain this information indefinitely. Nonpublic information that is no longer needed by the licensee should be destroyed in accordance with the licensee's record retention schedule and applicable law.**



**Question:** Independent of the provisions that apply to producers as licensees – are licensed agents/producers considered to be TPSPs for purposes of a licensee’s obligations under this section? Stated another way, do licensed producers have dual obligations as “licensees” and as “TPSPs”?

- The act defines “Third-party service provider” as “a person not otherwise defined as a licensee that contracts with a licensee to maintain, process, store or otherwise is permitted access to nonpublic information through its provision of services to the licensee.” Therefore, under the definition, a licensed agent or producer is not a TPSP.
- Section 38-99-70(A)(2) states that a Licensee who is an “employee, agent, representative or designee of a Licensee...is exempt from ...and “need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the other licensee.” This exemption requires an entire employee, agent, representative or designee to be fully covered by the program of another Licensee. Therefore, a Licensee who is an employee, agent, representative or designee of more than one other Licensee will only qualify for a Section 38-99-70(A)(2) exemption where the cybersecurity program of at least one of its parent Covered Entities Fully covers all aspects of the employee’s, agent’s representative’s or designee’s business.



**Question:** How will the information that is shared with other entities, states, regulatory agencies, and the NAIC under **38-99-60(C)(1)** be secured/protected against potential cyber security breaches?

**Section 38-99-60 affords this information confidential treatment and prescribes how this information may be shared. The South Carolina Department of Insurance is required by law to have an Information Security Program in place to protect confidential information filed by South Carolina consumers or SCDOI stakeholders.**





**Any Questions?**

**Please do not hesitate to  
contact the Department with  
additional questions at  
[datasecurity@doi.sc.gov](mailto:datasecurity@doi.sc.gov)**